Pentest Tools

# The audit bottleneck isn't policy. It's proof.

What 201 security and compliance practitioners told us about audit cycles, technical evidence, and the manual work automation was supposed to remove

A 2026 survey from Pentest-Tools.com

# Contents

01

# Foreword: the audit is annual. The evidence never stops.

Compliance has a reputation problem inside security teams. It gets described as paperwork, as a checkbox, as the thing that interrupts real work once a year. The data in this report tells a different story - and, honestly, a more demanding one.

We surveyed 201 security and compliance practitioners - IT managers, compliance and GRC leads, security engineers, DevSecOps professionals, and security specialists - about how their organizations maintain certifications like ISO 27001 and SOC 2. We went to the people doing the work rather than the executives, auditors, and governance teams who usually get asked, because no two compliance programs look alike and we wanted to see which pain points survive the differences.

What came back challenged our initial assumptions in the best way. The old picture - teams scrambling to assemble evidence in the weeks before an annual audit - is mostly gone. 60.2% of respondents assess their security controls at least monthly. 80.6% collect compliance evidence throughout the year. Nearly half discover control failures through continuous automated monitoring, long before an auditor would.

Continuous compliance, in other words, has already arrived. What hasn't arrived with it is the tooling underneath: only 38.3% rely primarily on automated evidence collection, and almost 9 in 10 still manually remap the same evidence across frameworks. The ambition went continuous; the labor stayed manual.

One respondent captured the daily reality behind those numbers:

> The hardest part is to automate the process. We usually provide the screenshots from the same menu over

and over to prove the system has not been changed.

So here is the thread running through every section that follows: the bottleneck in modern compliance isn't policy or paperwork. It's **producing technical evidence that security controls actually work**, at the pace environments change, without burning out the engineering teams who hold that evidence. Proof, not paperwork, is where the hours go.

Alongside the percentages, you'll find respondents speaking in their own words about what they would change if they could. Their answers carry the texture the numbers can't, so we've given them room. Use both to find where your own program sits in this picture, and where your evidence pipeline deserves attention first.

**Adrian Furtuna**
Pentest-Tools.com Founder & CEO

02

# Methodology and sample

Pentest-Tools.com surveyed 201 security and compliance practitioners in July 2026 via an online questionnaire. All respondents were screened for hands-on involvement in maintaining compliance certifications, and all could name the frameworks their organizations pursue.

Nearly 9 in 10 respondents maintain more than one framework. ISO 27001 and SOC 2 dominate, alongside PCI DSS, HIPAA, and a long tail of regional and sector-specific requirements.

**Organization size tested or secured**

**Fewer than 100 employees**
15.9%

**100 to 999 employees**
41.3%

**1,000 to 4,999 employees**
19.4%

**5,000+ employees**
18.9%

**Testing across multiple organization sizes**
4.5%

## What we asked

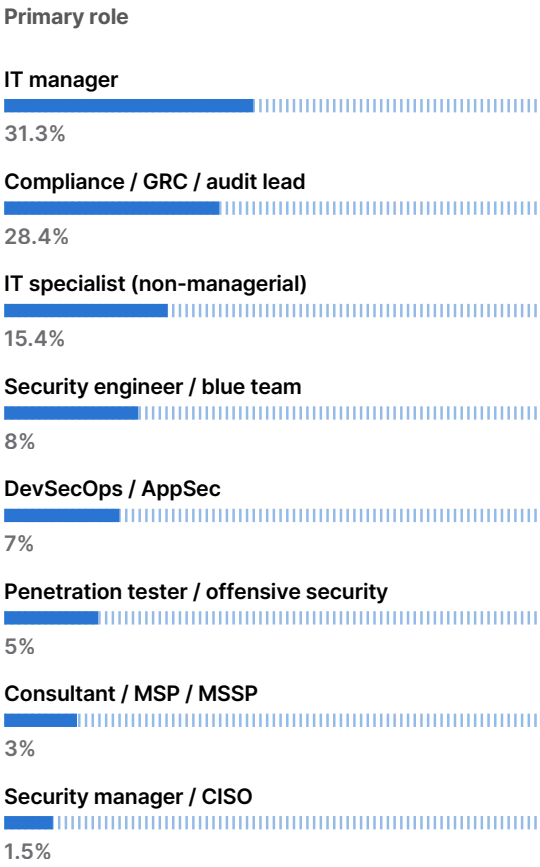
The questionnaire covered:

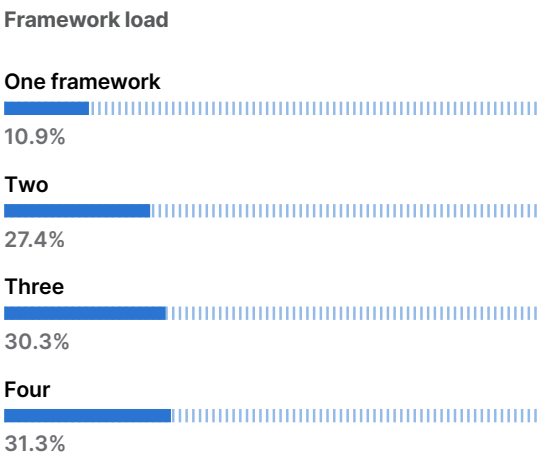
- → how often production environments change,
- → how often controls get assessed,
- → how evidence is maintained,
- → how control failures surface,
- → audit confidence,
- → the most time-consuming evidence activities,
- → cross-framework mapping effort, and
- → audit preparation bottlenecks.

A ranking question tested which tool and workflow factors matter most for audit readiness, and one open-ended question asked what practitioners would change if they could change one thing.

## How to read the numbers

All percentages refer to the full sample of 201 unless stated otherwise. Two questions (most time-consuming activities and audit bottlenecks) allowed up to three selections, so their percentages exceed 100 when summed. Organization-size splits involve modest subgroups and should be read as directional. Respondent quotes are lightly edited for spelling and grammar only; meaning is unchanged.



03

# Headline findings

Five results carry this report.
Read in sequence, as they describe a discipline whose ambitions went continuous while its labor stayed by hand.

1 **The annual compliance cycle is disappearing**

2 **Engineering capacity, not documentation, is what audits wait on**

3 **Evidence needs to cover the entire year; automation doesn't**

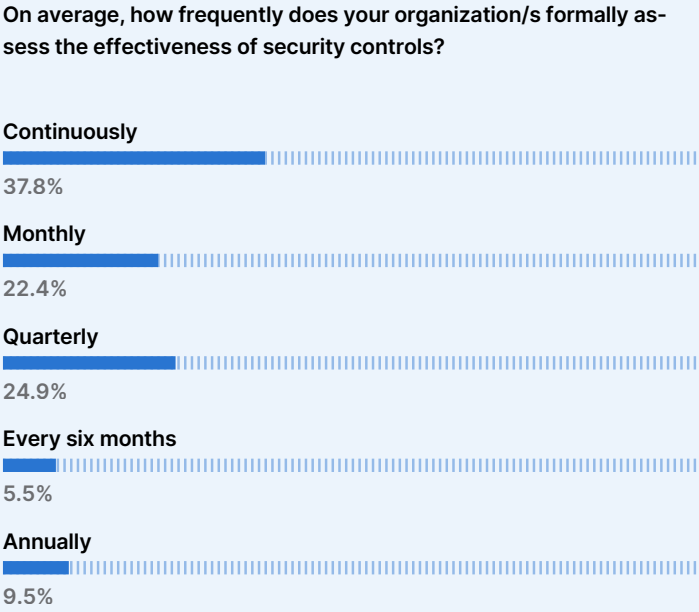
4 **Cross-framework mapping is where the duplication lives**

5 **Certification is trusted - with an expiry date**

1

## The annual compliance cycle is disappearing

60.2% of respondents formally assess the effectiveness of security controls at least monthly - 37.8% continuously, 22.4% monthly. Annual assessment survives in just 9.5% of organizations. The audit may still come once a year; the work no longer does.




2

## Engineering capacity, not documentation, is what audits wait on

Every top audit preparation bottleneck is operational: getting time and input from technical teams (50.7%), obtaining the required technical evidence (42.8%), coordinating across teams (36.3%), and resolving outstanding findings (34.3%).

3

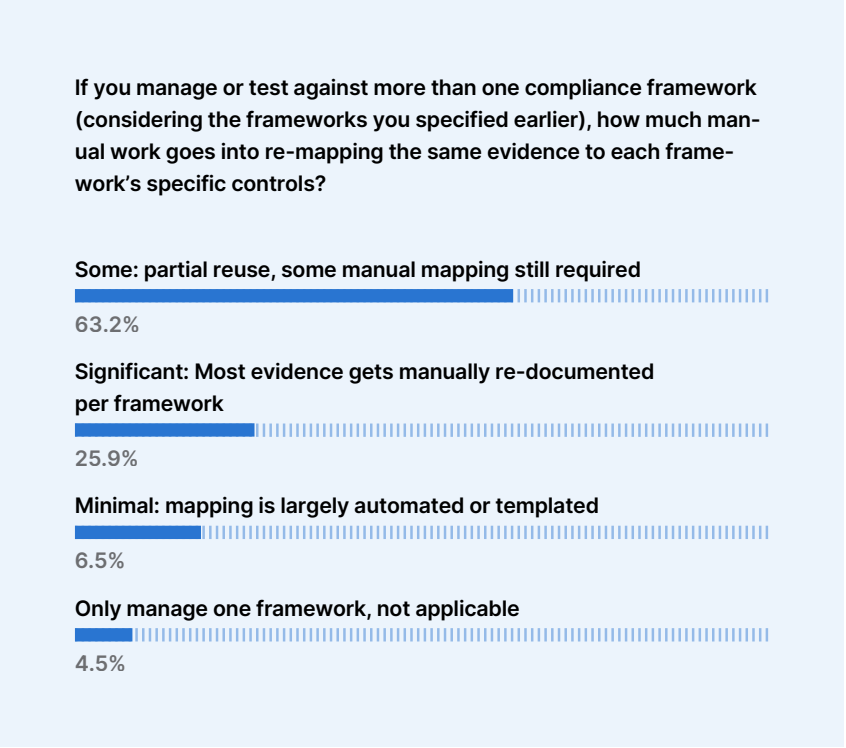
## Evidence needs to cover the entire year; automation doesn't

80.6% collect compliance evidence throughout the year, yet only 38.3% rely primarily on automated tooling - a plurality (42.3%) keeps continuous compliance alive through significant manual consolidation.


4

## Cross-framework mapping is where the duplication lives

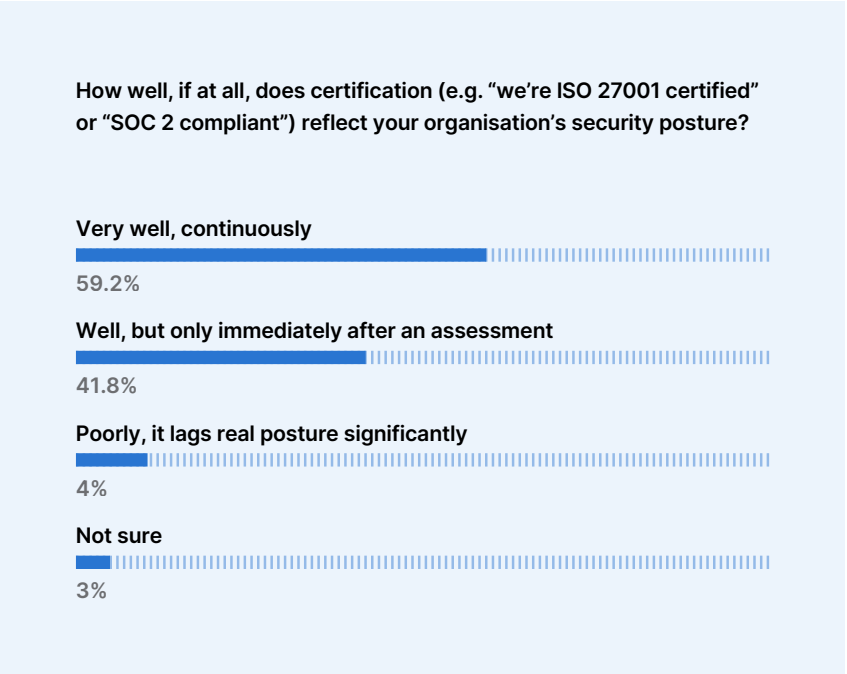
A mere 6.5% say tooling or templates handle most of the mapping between frameworks. 63.2% partially remap evidence by hand and 25.9% re-document the same evidence per framework - which puts manual mapping work at nearly 9 in 10.



5

## Certification is trusted - with an expiry date

93% believe certification reflects their security posture, but only 51.2% believe it does so continuously; 41.8% say it's accurate only immediately after an assessment. That belief predicts audit confidence almost linearly: 59.2% of the "continuous" camp would be very confident in a next-day audit, versus 16.7% of the "only right after" camp.




Connect the five and the causal chain shows itself. When security assessments went continuous, they multiplied the evidence to produce. The production stayed manual, which made technical teams the choke point. And because the evidence trail decays between audits, confidence in the certification decays right along with it.

> Teams are stretched all across the organization, and the perception is that this is all my team's job, but it's the responsibility of everyone.
>
> Those with more technical roles tend to deprioritize any audit work until it becomes urgent.

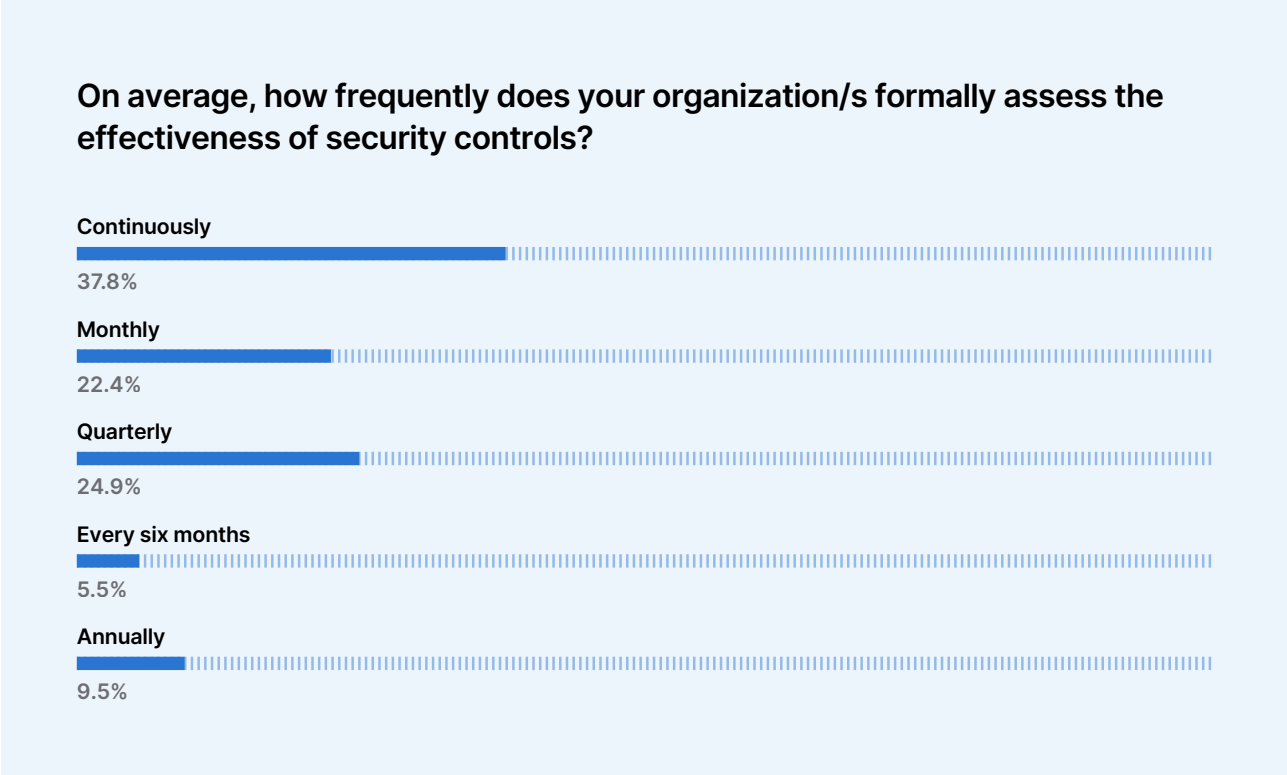
None of that is a paperwork problem. It's what continuous ambition looks like when the proof-producing machinery hasn't kept up.

04

# Assessment has outpaced change

Going in, we assumed most organizations would assess security controls annually or quarterly, in step with their audit calendars.

The data says otherwise: 37.8% assess continuously, another 22.4% monthly - 60.2% checking controls at least once a month - and only 9.5% still work on an annual rhythm. Nobody in the sample assesses less often than that.

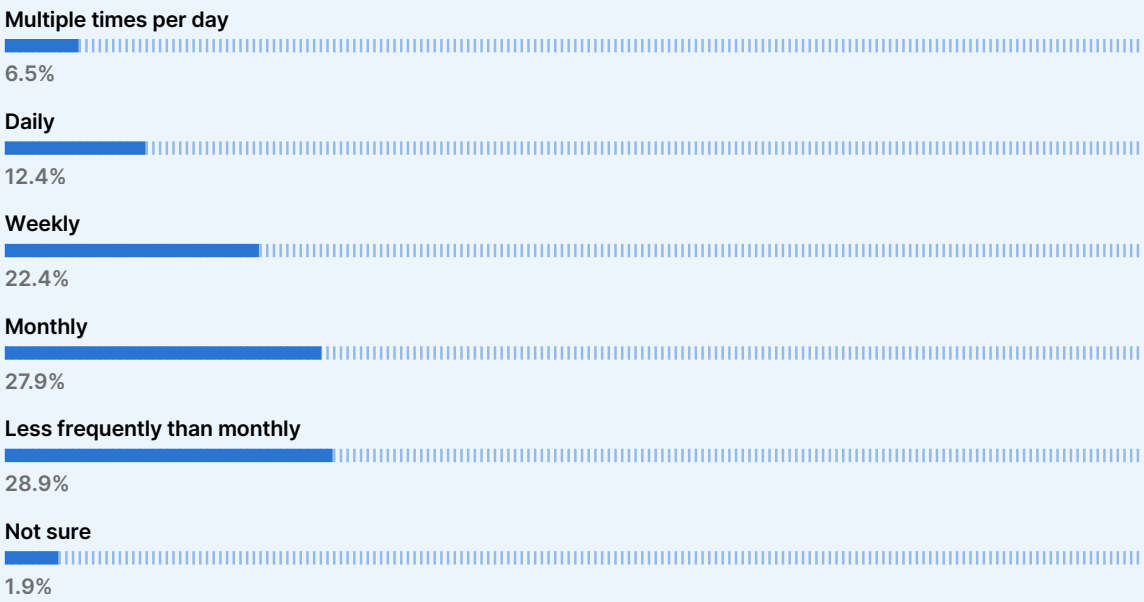



## Assessing systems faster than they change

Now hold that against how often things actually change. More than half of respondents (56.8%) say their production environments change monthly or less frequently - 27.9% monthly, 28.9% less often still. Which means a striking number of organizations now assess their controls as often as, or more often than, their environments change.

**On average, how frequently do production systems or applications within your organisation/s change?**

Change cadence VS assessment cadence, n=201



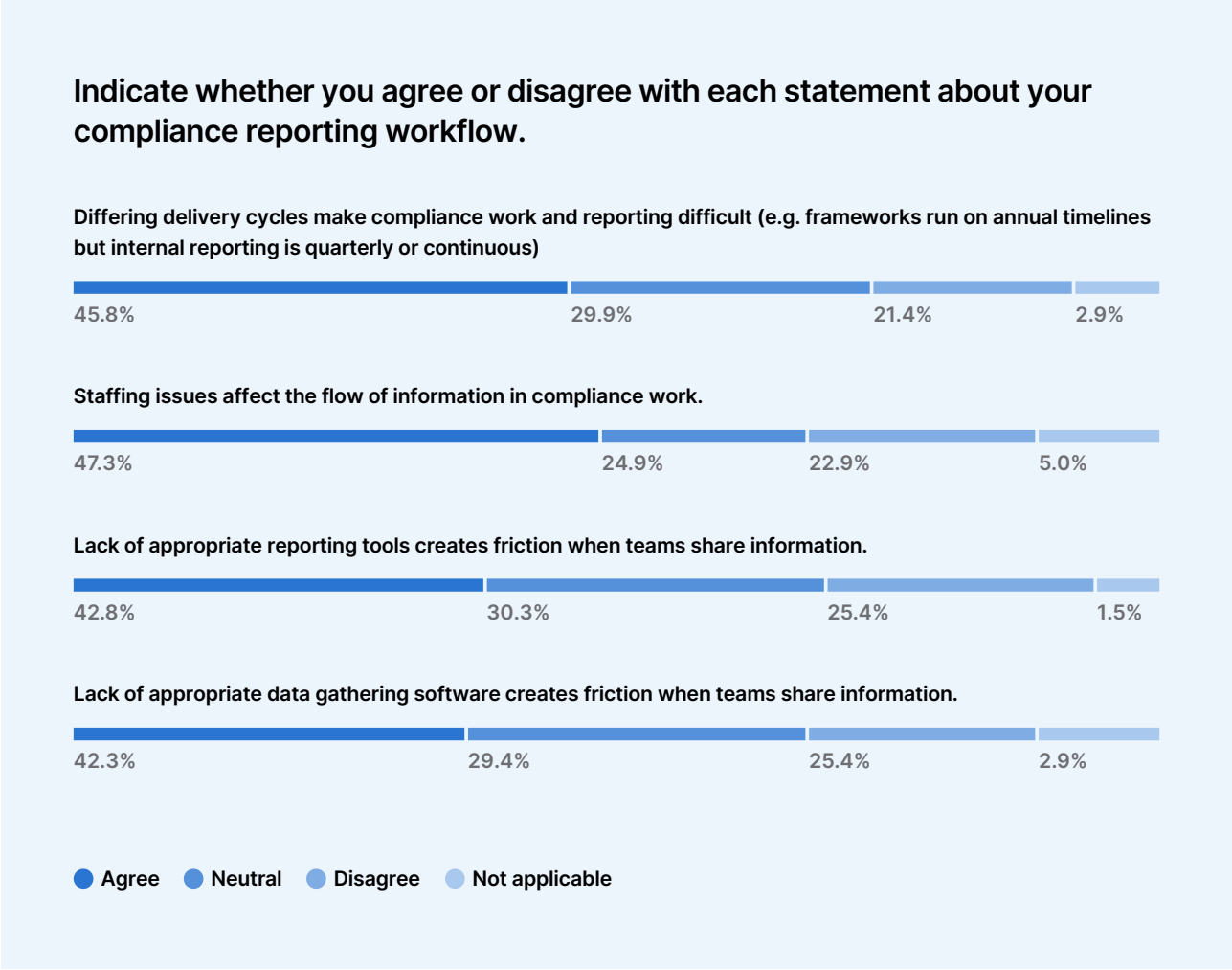

There are two honest readings, and they probably both hold.

- → The generous one: **continuous assessment is ahead of the game** - these organizations have decoupled checking from deploying, treating control validation as an always-on discipline rather than a reaction to change.
- → The cautious one: **some teams assess more than their rate of change strictly demands, pushed from outside**. And the outside pressure is real - the volume of publicly disclosed and actively exploited vulnerabilities keeps climbing, which means an environment can become exposed without changing at all. A control that passed last month can fail this month because the world around it moved.

Whichever reading you prefer, the practical consequence is identical: assessment at this cadence generates evidence at a pace that annual audit processes were never designed to absorb.

## The friction is measurable

We asked directly whether mismatched cadences hurt. 45.8% agree the mismatch makes compliance work difficult, and only 21.4% disagree. Staffing scores even higher, with 47.3% agreeing that staffing issues disrupt the flow of compliance information, while 42.8% point to reporting tools and 42.3% to data gathering software.




> Change the way the other teams handle their work. Our side is always up to date, running. Other teams take days to even reply.

The compliance cycle went continuous. What follows is about what that costs - and who pays it.

05

# Technical evidence, not policy, is the bottleneck

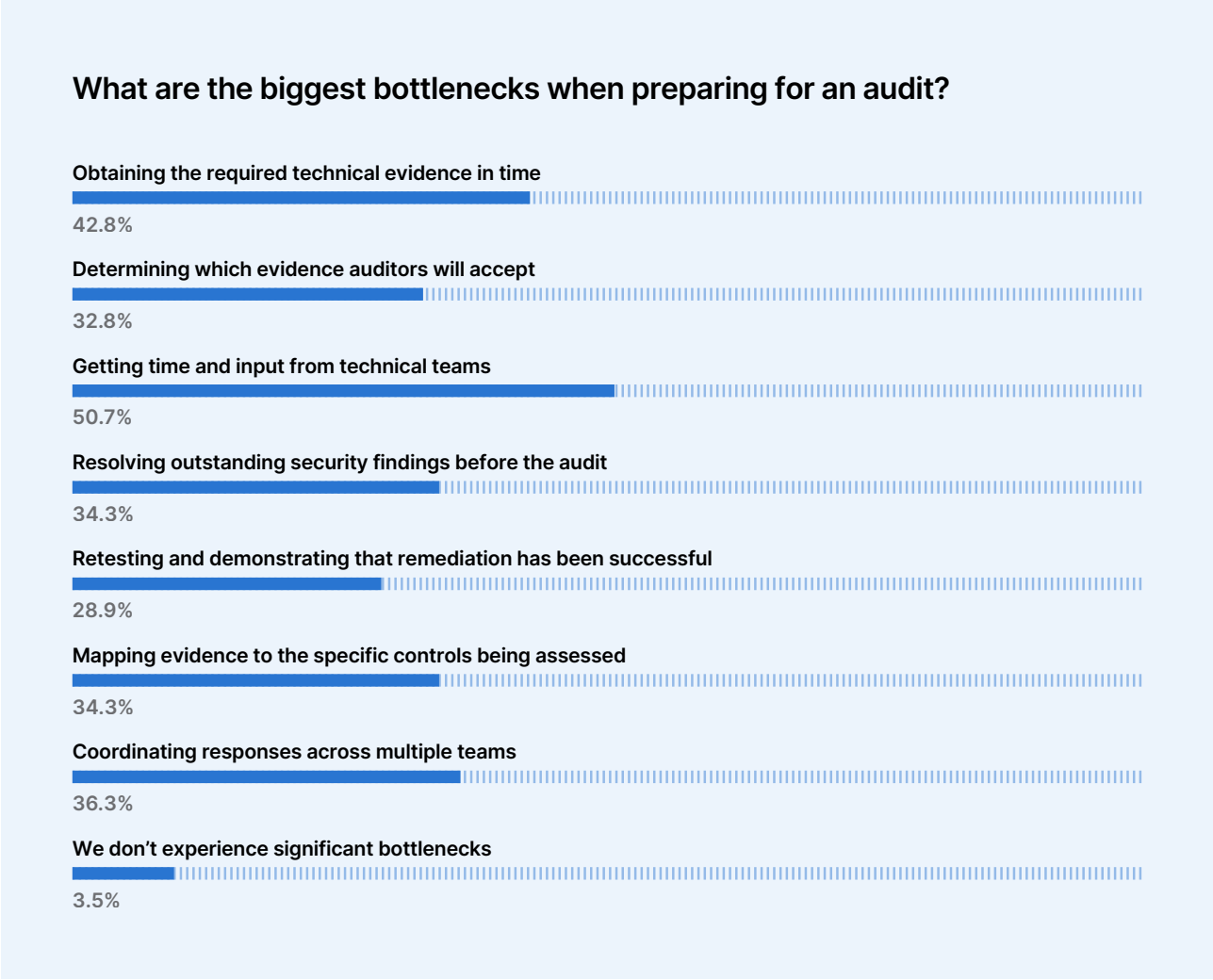

Ask what slows audits down and the traditional answer is documentation: policies, procedures, the paperwork layer. The respondents point somewhere else entirely.

Their biggest audit preparation bottlenecks (up to three selections):

- → Getting time and input from technical teams: 50.7%
- → Obtaining the required technical evidence in time: 42.8%
- → Coordinating responses across multiple teams: 36.3%
- → Resolving outstanding security findings before the audit: 34.3%
- → Mapping evidence to the specific controls being assessed: 34.3%
- → Determining which evidence auditors will accept: 32.8%

→ Retesting and demonstrating successful remediation: 28.9%

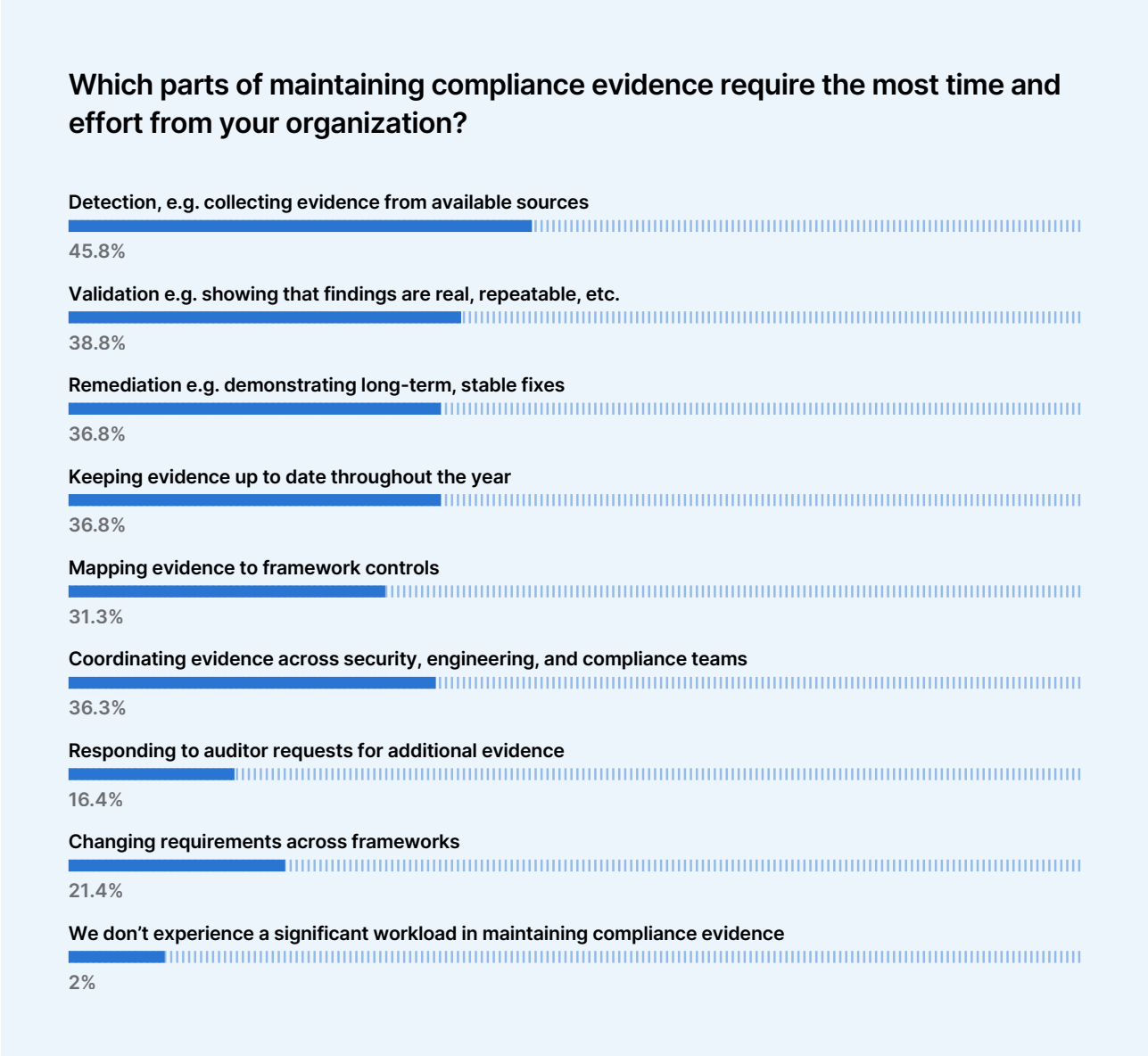
Only 3.5% report no significant bottlenecks at all.




Notice what every top answer has in common: they're all about engineering capacity. Audits don't stall on policy writing - they stall on the time of the people who hold the technical evidence, the effort of extracting it, and the work of proving that findings were real and fixes held.

## Collecting proof is harder than fixing problems

The same shape repeats in the question about time. Detection - collecting evidence from available sources - tops the list of most time-consuming activities at 45.8%, ahead of validation, showing that findings are real and repeatable (38.8%), and remediation, demonstrating stable fixes (36.8%). Keeping evidence current through the year (36.8%) and coordinating it across teams (36.3%) sit right behind.




Sit with that for a second: collecting proof outranks fixing problems. And just 2% of respondents say maintaining compliance evidence isn't a significant workload.

This is the survey's center of gravity, so let's state it plainly. Security teams mostly already have the information auditors need - the scans run, the controls exist, the fixes ship. The bottleneck is turning what they know into what they can show: proof that a control works, that a finding was real, that a fix held. Detection alone proves nothing to an auditor. The distance between "we know" and "we can show" is where the hours, and the engineering goodwill, drain away.

> Fully automate evidence gathering and mapping to stop wasting weeks manually pulling data and chasing engineering teams before audits.

06

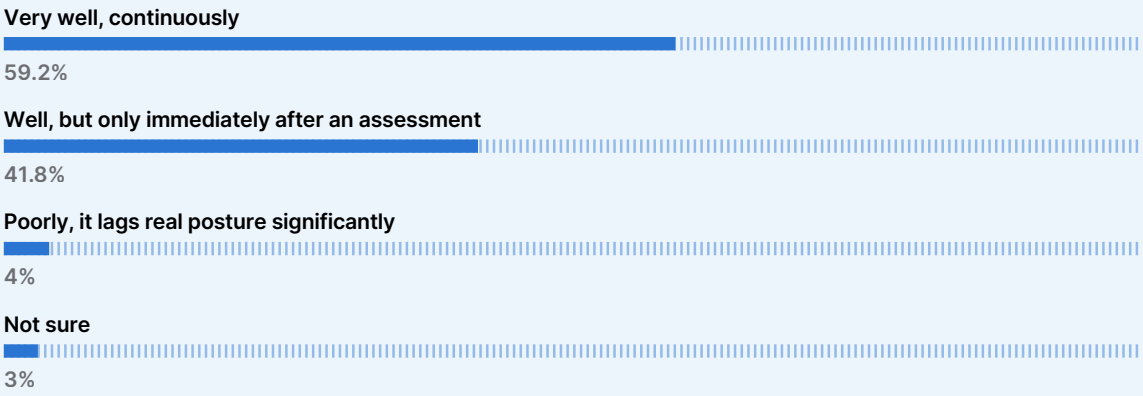
# Certification's expiry date

93% of respondents believe certification reflects their organization's security posture. On its own, a strong endorsement. The interesting part is the qualifier that nearly half of them attach.

51.2% say certification reflects posture continuously. 41.8% say it depicts reality well - but only immediately after an assessment. Just 4% call it a poor reflection outright.

Certification isn't distrusted, then; it's trusted with an expiry date. Almost half the practitioners maintaining these certifications believe the badge is accurate on assessment day and fades from there.

**How well, if at all, does certification (e.g. "we're ISO 27001 certified" or "SOC 2 compliant") reflect your organisation's security posture?**

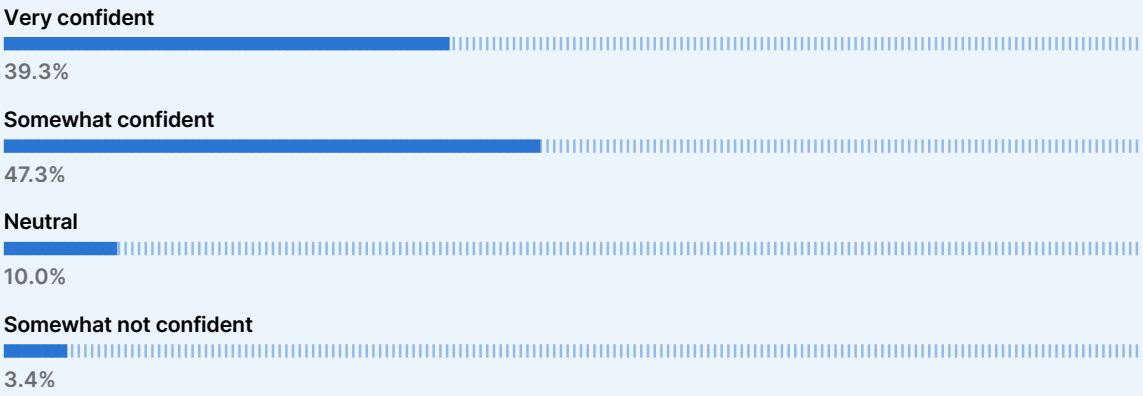



## Belief in the badge predicts confidence in the audit

Among those who believe certification continuously reflects posture, 59.2% would be very confident demonstrating control effectiveness in a surprise next-day audit. Among those who believe it's accurate only immediately after an assessment, just 16.7% share that confidence.

**How confident are you that your tested organization/s could demonstrate the effectiveness of security controls if an audit took place tomorrow?**

Confidence in demonstrating control effectiveness in a next-day audit, n=201




Confidence between audits doesn't come from the certificate; it comes from continuing to validate controls and produce current technical evidence as the environment changes. The people who believe their certification stays accurate are, by and large, the people whose evidence stays up to date. The ones watching it decay are describing their own evidence pipeline as much as the badge.

Step back and the pattern is preparedness without certainty: 86.6% are at least somewhat confident they'd pass a next-day audit, but only 39.3% are very confident.
What separates them is evidence.

> Better automation, experienced resources, tone at the top change so that management sees certification and compliance process as an integral part of the organization and not as a tick-the-box item or a badge for advertisement.

07

# Continuous evidence, manual muscle

80.6% of respondents maintain compliance evidence throughout the year. That confirms the continuous-compliance story - until you look at **how they do it**.

38.3% rely primarily on automated security tooling. 42.3% collect continuously but depend on significant manual consolidation. Another 14.9% still assemble evidence before audits, and 4.5% get it from engineering teams on request.


In other words, the largest single group runs continuous compliance on human effort - someone exporting, screenshotting, consolidating, and formatting, all year long. The norm arrived before automation did.

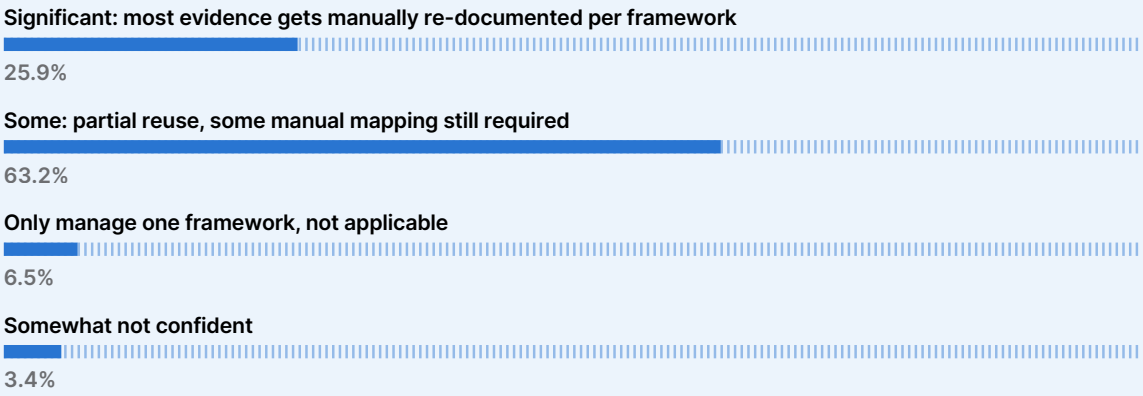
## Multiply by every framework

The manual work compounds wherever frameworks overlap - and nearly 9 in 10 respondents maintain more than one. Only 6.5% say tooling or templates handle most of the evidence mapping between them. 63.2% partially remap evidence by hand, and 25.9% mostly re-document the same evidence per framework.

Almost 90%, then, still perform manual mapping work, much of it duplicative: the same scan result, the same control, proven separately for ISO 27001, SOC 2, and whatever else the organization holds.

**If you manage or test against more than one compliance framework (considering the frameworks you specified earlier), how much manual work goes into re-mapping the same evidence to each framework's specific controls?**

Manual work in cross-framework evidence mapping, n=201



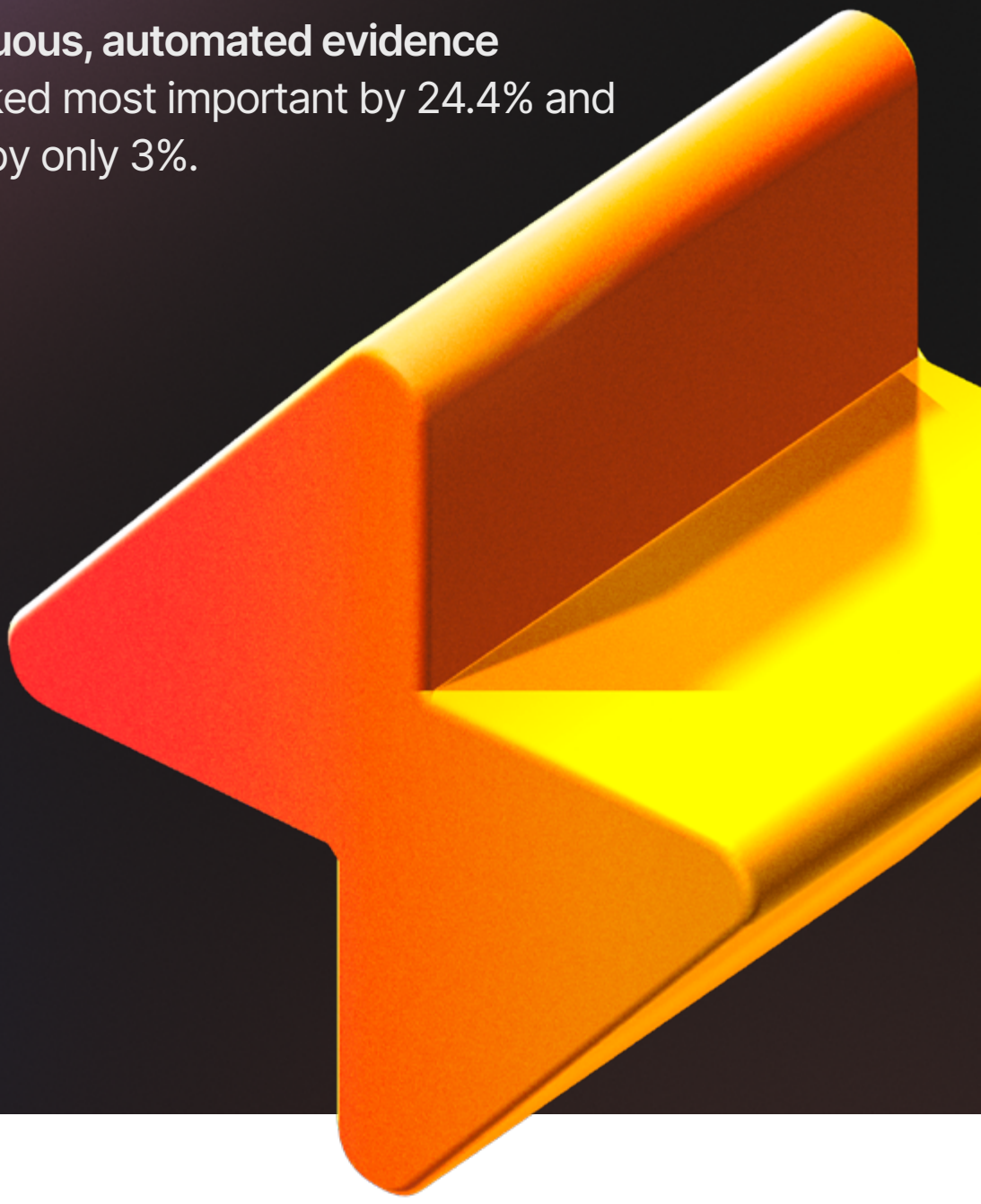

> I'd like the process of gathering evidence for compliance audits to be far more automated. Right now, mapping controls and pulling together proof between audit cycles takes a lot of repetitive manual work, and a system that generated and organized that evidence continuously would save significant time and reduce the risk of human error.

Step back across sections 05 through 07 and one consistent picture emerges: organizations committed to continuous compliance before their tooling did. The result is an always-on process powered by manual labor - the kind of arrangement that works right up until the people carrying it burn out or move on.

08

# What practitioners want fixed first: less manual work, not more integrations

We asked respondents to rank seven factors by how much they matter when evaluating tools and workflows for audit readiness. The winner was decisive: **continuous, automated evidence generation**, ranked most important by 24.4% and least important by only 3%.



Integration with existing GRC and ticketing tools tells the opposite story. Only 12.9% ranked it most important - and it drew the second-highest “matters least” score of all seven factors (7.5%, behind only cost). Forced to choose, practitioners didn’t merely rank integration lower than automation. They actively pushed it down the list.

## When evaluating tools or workflows to support audit readiness, which factors matter most?

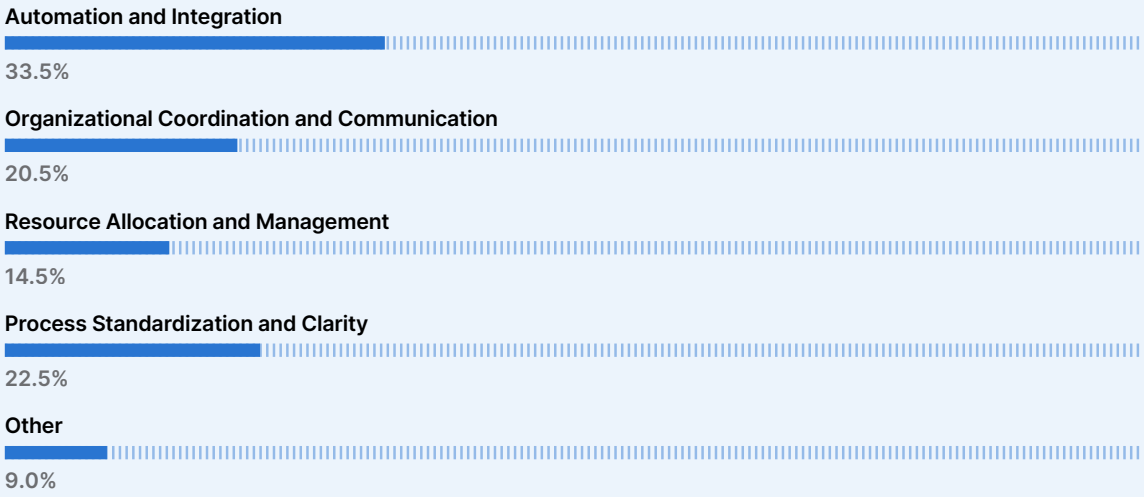
Share ranking each factor as mattering most, n=201

## The paradox to investigate further

Here's what makes this genuinely interesting: in the open-ended responses, integration is among the most-mentioned requests. Automation and integration together dominate the "change one thing" answers, at 33.5% of all responses. People say they want integrated platforms - then rank integrations near the bottom when priorities get forced.

**If you could change one thing about your workflows, bottlenecks, and experiences with regards to certification processes, what would it be?**

What practitioners would change first, coded from open-text responses, n=201




The resolution probably lives in what "integration" means to the people asking for it. Read the verbatims closely and the request is rather for one place where evidence lives, stays current, and maps to controls without being reassembled by hand. Practitioners are describing an outcome (a single, continuously maintained evidence base), not a mechanism (tool-to-tool plumbing).

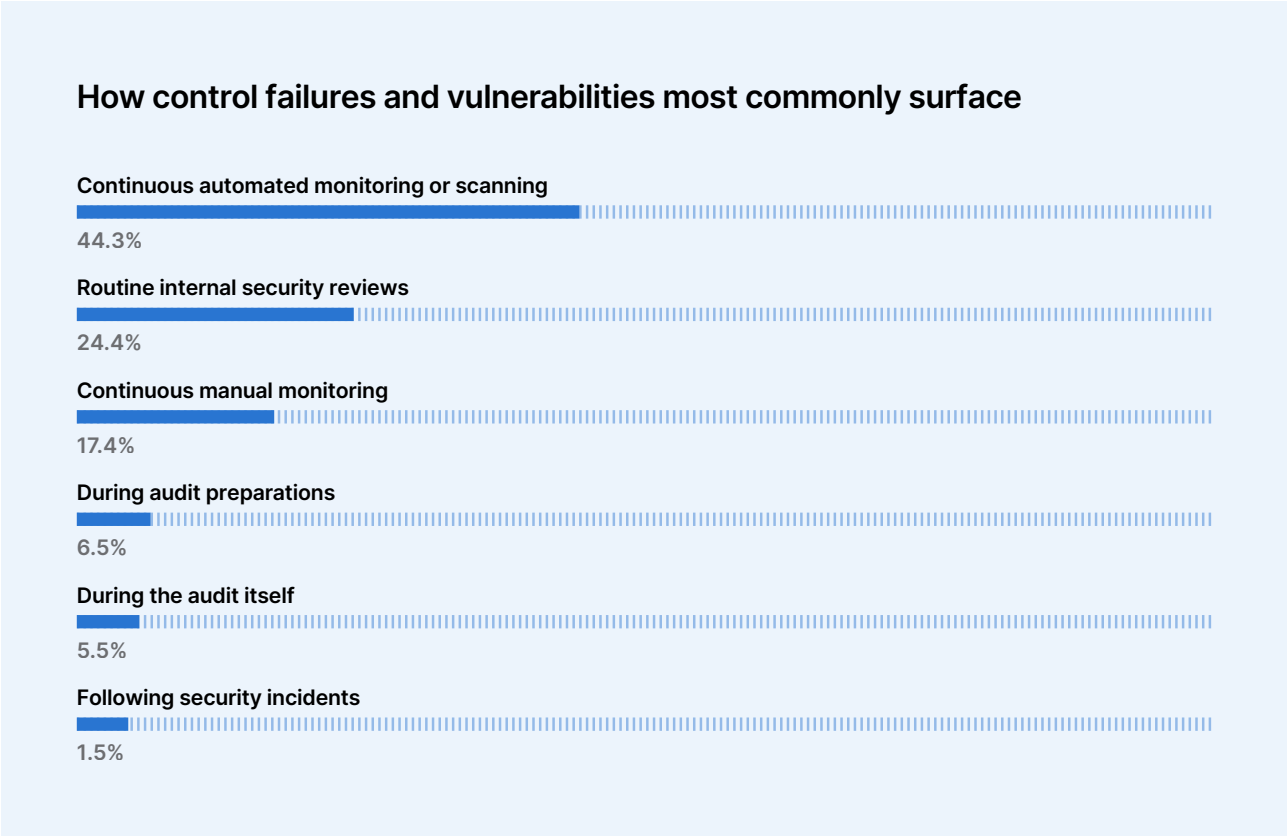
> If I could change one thing, it would be shifting from manual, point-in-time evidence gathering to automated, continuous control monitoring with cross-framework mapping.

The signal for anyone building or buying in this space: cutting manual work beats connecting more tools. Another connector that still needs a human to consolidate the output doesn't touch the problem practitioners ranked first. Evidence that generates and organizes itself does.

09

# Finding failures before the auditor does

One hypothesis behind this survey was that organizations mainly discover control failures during audit preparation or the audit itself - the “scramble” model. The data firmly rejects it.




Only 12% of organizations first learn about their failures from the audit process. The overwhelming majority surface issues themselves, through monitoring and review that runs all year - the healthiest finding in the survey, and the strongest confirmation that compliance has genuinely gone continuous.

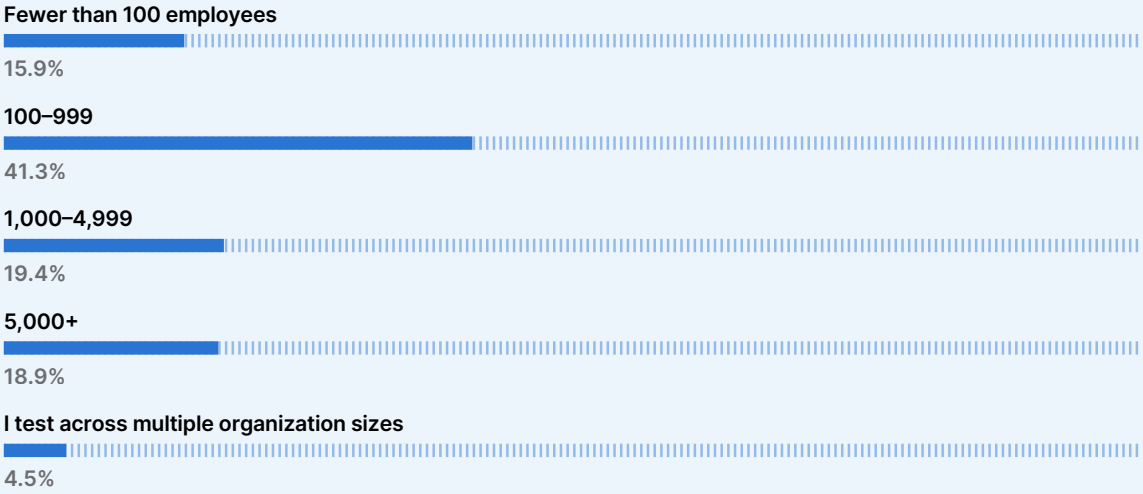
## Size and maturity shape the picture

Split the discovery data by organization size and a maturity gradient appears. Among organizations under 100 employees, 31.3% discover failures through continuous automated monitoring - and nearly 1 in 5 still first encounters issues during audit preparation or the audit itself. In the 100-to-999 band, automated discovery rises to 44.6%. Past 1,000 employees, it reaches roughly half.

With their more mature processes and longer-established tooling, **large organizations lean hardest on automated discovery**; the smallest remain most dependent on the audit cycle to surface problems. (The size subgroups are modest, so read this as a directional pattern rather than a precise ladder - but its direction matches everything else in the survey.)

## How large is/are the organization/s you primarily test or secure?

Automated discovery rises with organization size, directional, n=201




For smaller teams, there's encouragement hiding in that gradient. What separates them from the enterprises isn't headcount - it's machinery. And automated discovery is the one rung of this maturity ladder that doesn't require a bigger team to climb.

# Closing the evidence gap with validation that holds up

Nothing in this survey suggests the pressure eases from here. Assessment cadences will keep tightening, evidence volume will grow, frameworks will continue to multiply. The variable that can change is how much of that evidence comes from automated tools instead of tired humans with screenshot folders.

This is **where Pentest-Tools.com fits**. No single tool removes the compliance workload this survey describes, and we won't pretend otherwise. What we've built targets the bottleneck practitioners identified: **producing technical evidence that security controls work**, without another round of chasing engineering teams.

## Evidence built into the testing, not assembled after

Most security tools stop at detection: they tell you something might be wrong, then leave you to prove if it's real, fixed, and if an auditor might care. But detection alone proves nothing - to an attacker or to an auditor.

This is the gap vulnerability validation closes. It's the category of tools that confirm which detected issues are actually exploitable - by exploiting them safely, capturing evidence of what the exploit reached, and re-testing once a fix lands.

**Pentest-Tools.com combines detection and validation in one workflow**, across web, network, API, and cloud, with evidence you can hand to developers, IT, leadership, or an auditor.

## Up to date proof you can reference anytime

Pentest-Tools.com marks a finding Confirmed only after proving it's exploitable, and every Confirmed finding arrives with the evidence already attached:

- → **Request and response pairs** - exactly what the exploit sent and what came back, timestamped, so an auditor can see where and when the control failed.
- → **Extracted artifacts** - the usernames, passwords, or files the exploit actually reached.
- → **Attack replay** - reproduce the finding on demand, so proving a fix held is a re-run rather than a fresh investigation.

Sniper: Auto-Exploiter produces that evidence automatically for high-impact CVEs, while the ML Classifier filters likely false positives before they reach your queue.

That's the difference between "potentially vulnerable Apache version" and a confirmed exploitation path with the proof attached.

## Built for the cadence you already run

With 60.2% of organizations assessing controls at least monthly, the workflow for producing evidence has to keep that pace too. Vulnerability monitoring runs scheduled assessments against your systems, captures what changed between runs, and routes validated findings into Jira, Vanta, or wherever remediation already happens. Retesting captures before-and-after evidence automatically, so 'proving a fix works' is part of the workflow, not as a separate project.

## What this means in practice

A team that needs to maintain two or three frameworks can put scans on schedule and get validated findings instead of assembling manual proof. Remediation evidence accumulates as fixes ship, so pre-audit work becomes a review, not reconstruction. The bottleneck at the top of the survey (getting time from technical teams, at 50.7%) shrinks, because the evidence that used to cost an engineer's afternoon now gets automatically captured at test time.

We won't claim this covers every framework control - policy, HR, and physical controls still need their own evidence. But technical controls are where this survey says the time and friction go. Automate the proof for those, and continuous compliance becomes something you do, not something you struggle with.

**See how we support specific compliance frameworks**

# Before you act on this report

Two kinds of questions tend to follow findings like these: what the data can honestly support, and what it implies for choosing tools. They deserve separate treatment, because the first set is answered by the survey and the second by our experience building for this problem.

## What the data can and can't tell you

**"Does this mean annual audits are becoming irrelevant?"**

No - it means the annual audit is becoming the checkpoint on a continuous process rather than the process itself. 60.2% of organizations already assess controls at least monthly, and only 12% first discover failures through the audit cycle. The audit still matters for trust and market access; it just no longer describes how the work happens.

**"Is manual evidence work really that universal, or just badly distributed?"**

Close to universal. Only 2% say compliance evidence isn't a significant workload, only 3.5% report no audit bottlenecks, and only 6.5% have largely automated cross-framework mapping. Intensity varies with framework count and organization size, but essentially everyone in the sample carries some of the load.

**"We're a small team. Are we just behind the big companies?"**

On process maturity, somewhat - larger organizations lean more on automated discovery, while the smallest still surface more issues during audit prep. But the gap is machinery, not headcount. Automated monitoring and evidence capture are the parts of the maturity curve that don't require more people, which makes them the highest-value starting point for a small team.

## Choosing tools in light of this

**“Should we prioritize GRC integration or automated evidence generation?”**

The survey’s answer is unambiguous: forced to rank, practitioners put continuous automated evidence generation first (24.4% ranked it most important) and integration near the bottom (12.9%, with the second-highest “matters least” score). The open-text answers reveal the deeper wish - a single, continuously current evidence base, not more connectors. Buy the thing that removes manual work first, then integrate it where remediation already happens.

**“How does validated testing evidence actually help in an audit?”**

Auditors accept evidence that shows a control worked at a point in time, that findings were real, and that fixes held. A validated finding carries that story natively: proof of exploitability, a tracked remediation, and a retest with before-and-after artifacts. Unvalidated scanner output invites the question teams dread - “can you show this was real and is now fixed?” - which sends someone back to the engineering queue.

**“Won’t continuous testing just create more findings to manage?”**

More findings, yes - but validated ones, prioritized by proven exploitability, arriving steadily instead of in a pre-audit avalanche. The avalanche model is what breaks teams: evidence collection already outranks fixing problems as the top time sink. A steady, validated flow is precisely what makes the workload manageable.

# Vulnerability validation. Because detection alone proves nothing.

If there’s one thing this survey should retire, it’s the image of compliance teams scrambling once a year. The practitioners here are ahead of their tooling - running continuous assessment and year-round evidence collection on sheer manual effort, finding their own failures long before an auditor would.

They have the discipline. What they lack is a way to turn what se-

curity teams already know into what auditors can accept, without borrowing another afternoon from engineering.

Only you can decide where to start in your own environment. But **201 of your peers just showed you where the pressure concentrates**: in the gap between knowing a control works and proving it, again and again, for every framework you hold. Start with one question: how much of your evidence still gets made by hand?

# Pentest-Tools.com

## Security findings you can prioritize.
## In web apps, network, and cloud.

Pentest-Tools.com is the only vulnerability validation product that combines detection and validation in one workflow across web, network, and cloud targets - with evidence practitioners can hand directly to developers, IT, leadership, and auditors.

It discovers security issues across **web, network, and cloud** targets and **validates** them automatically in the same workflow. When it proves exploitability, it marks the finding as Confirmed, backs it with **evidence** - such as valid credentials, file access indicators, and screenshots - and lets the practitioner replay the attack.

Unlike legacy scanners that stop at detection and leave practitioners to prove exploitability by hand, Pentest-Tools.com validates as it tests - keeping the practitioner in full control of every stage with deterministic capabilities and automating for efficiency, depth, and speed with AI only where it makes sense.

With Pentest-Tools.com in their workflow, security and IT teams spend less time on manual triage - and walk away with findings they can defend to leadership, auditors, developers, and IT, and a basis for prioritizing remediation on proven risk, not theoretical severity.

Discover more on **pentest-tools.com/product**

Pentest Tools

Europe, Romania, Bucharest
48 Bvd. Iancu de Hunedoara
support@pentest-tools.com
Pentest-Tools.com

Join our community on:
LinkedIn | Youtube | Reddit